# DESCENT ON SUPERELLIPTIC CURVES

MICHAEL MOURAO

Abstract. We are concerned with the question of determining the set $C(\mathbb{Q})$, where $C$ is a curve defined by an equation of the form $y^q = f(x)$, where $q$ is an odd prime and $f$ is a polynomial defined over $\mathbb{Q}$. This question can often be answered using a set which encapsulates information about local solubility of a particular collection of covers of $C$. We define this set and show how to compute it.

## 1. Introduction

When working with the set of rational points $C(\mathbb{Q})$ of an algebraic curve $C$, we often encounter examples where the Hasse principle fails to decide whether this set is empty or not. The method of two-cover descent on hyperelliptic curves is based on the fact that, for a hyperelliptic curve $C$, there is a computable collection of covers $\phi_\alpha : D_\alpha \to C$, such that

$$C(\mathbb{Q}) = \bigcup_{\alpha \in \text{finite set}} \phi_\alpha(D_\alpha(\mathbb{Q})). \tag{1.1}$$

Therefore, when local-to-global arguments cannot be applied directly to $C$, the problem can be transferred to the one of looking for rational points on the covers. This is described explicitly in [6]. In the present paper we extend this method to superelliptic curves $C$ defined by an equation of the form $y^q = f(x)$, where $q$ is an odd prime and $f \in \mathbb{Q}[x]$ is $q$-th power-free. The theory behind the process of performing descent on the Jacobian variety $J_C$ of such curves, defined over a field containing the relevant roots of unity, is studied in detail in [12]. In [7], an extension of the descent map to the Picard group of curves of this type is used to introduce new insights on the nature of Ш$(J_C/\mathbb{Q})$. Nevertheless, it is often much simpler and faster to avoid working with the rational points of the Jacobian and instead restrict to information obtained using only the initial curve. The Selmer set we define contains information which is sometimes sufficient to determine the set $C(\mathbb{Q})$. We explain the necessary theory and present an explicit algorithm, similar to the one in [6], to compute this Selmer set. Note that we can not use a trivial extension of the existing routines because our algorithm is expected to deal with the possibility of singular points, which do not appear in the case of hyperelliptic curves.

The problem of finding points on superelliptic curves generalizes the problem of finding solutions to Thue equations (see [10]) and can also be used to solve generalized Fermat equations. In Example 4.2 we solve four such equations considered in [9], which were used by the authors as examples of the limitations of their approach. Thus in many situations descent arguments are more appropriate than other techniques. As illustrated by Examples 4.1 and 4.2 it is often the case that $C$ is everywhere locally soluble, but its associated covers fail to be so, preventing $C$ from having any rational points, since the union in (1.1) is comprised of empty sets. In Example 4.3, local information together with information obtained using subcovers, following a method proposed in [4] and [5], is used to prove that the curve

$$y^3 = (x^2 - 3)(x^4 - 2)$$

2010 *Mathematics Subject Classification.* Primary 11G30 ; Secondary 11G20, 11D41, 11D45.

The author is supported by the research grant FCT SFRH/BD/44011/2008.

has no rational points except from one rational point at $\infty$. By making descent applicable to singular superelliptic curves, we were able to prove in Theorem 4.5 that the only pair $(a,b)\in\mathbb{Z}^2_{>0}$ satisfying

$$b^3=\sum_{i=1}^{a} i^9$$

is $(1,1)$.

## 2. Descent on superelliptic curves

### 2.1. Preliminaries.

**Definition 2.1.** Let $q$ be an odd prime and $n$ be a positive integer. We define a **superelliptic curve** to be a plane curve $C$ defined as the locus of the equation

$$y^q=f(x)=a_nx^n+\ldots+a_1x+a_0,$$

for some polynomial $f$ with coefficients in $\mathbb{Q}$.

*Remark* 2.2. When $q\nmid n$ we think of $C$ as having a single point at infinity, otherwise $C$ has $q$ distinct points at infinity.

**Proposition 2.3.** *Every superelliptic curve is birational to a superelliptic curve satisfying an equation of the form $y^q=f(x)$, where $deg(f)=n$ and $q\mid n$.*

*Proof.* Suppose $C':(y')^q=f'(x')$ is a superelliptic curve and that $\deg(f')=m=iq+j$ with $i\in\mathbb{Z}_{\geq 0}$ and $0\leq j<q$. Pick $\alpha\in\mathbb{Q}$ such that $f'(\alpha)\neq 0$. Define the polynomial $h$ by $f'(x')=h(x'-\alpha)$ and the polynomial $f$ of degree $n=q(i+1)$ by $f(x)=h(1/x)x^{q(i+1)}$. Let $C$ be the superelliptic curve defined by $y^q=f(x)$. Then $C'$ is birational to $C$ via the map $(x',y')\mapsto\left(\frac{1}{x'-\alpha},\frac{y'}{(x'-\alpha)^{i+1}}\right)$. $\square$

In light of this proposition, we will assume that $a_n\neq 0$ and that $q\mid n$ throughout the rest of the paper. When this holds, we can also think of $C$ as being the locus of the equation

$$Y^q=F(X,Z)=a_nX^n+\ldots+a_1XZ^{n-1}+a_0Z^n \tag{2.1}$$

in the weighted projective plane $\mathbb{P}^2(1,\frac{n}{q},1)$, where the variables $X$ and $Z$ have weight 1 and $Y$ has weight $n/q$. We will be using the affine and projective descriptions of $C$ interchangeably. Without loss of generality, we may assume that $f$ is a $q$-th power-free polynomial with integer coefficients.

From now on let $\Bbbk$ denote one of $\mathbb{Q}$, $\bar{\mathbb{Q}}$, $\mathbb{Q}_p$, $\bar{\mathbb{Q}}_p$ (where $p$ can be any rational prime). Define $\mathcal{F}_\Bbbk$ to be the set of monic, irreducible over $\Bbbk$, polynomials such that

$$f=a_n\prod_{h\in\mathcal{F}_\Bbbk}h^{n_h},$$

where $1\leq n_h\leq q-1$ for all $h\in\mathcal{F}_\Bbbk$. Denote the degree of $h$ by $d_h$. Let $A_\Bbbk$ be the semi-simple $\Bbbk$-algebra $\Bbbk[t]/(g(t))$, where

$$g=\prod_{h\in\mathcal{F}_\Bbbk}h.$$

Note that $g$ is defined over $\mathbb{Q}$ and does not depend on $\Bbbk$. We denote its degree by $d$. $A_\Bbbk$ decomposes as a direct product of finite field extensions of $\Bbbk$

$$A_\Bbbk=\prod_{h\in\mathcal{F}_\Bbbk}K_h=\prod_{h\in\mathcal{F}_\Bbbk}\Bbbk[t]/(h).$$

Denote by $\theta_h\in K_h$ the image of the generator $t$ under the quotient map and by $\Theta_\Bbbk$ the set

$$\Theta_\Bbbk=\{\theta_h\quad:\quad h\in\mathcal{F}_\Bbbk\}.$$

For the following definition we will assume that a point $(X,Y,Z)\in C(\Bbbk)$ is normalized such that if $\Bbbk=\mathbb{Q}$ then $X,Y,Z\in\mathbb{Z}$ with $\gcd(X,Z)=1$ and if $\Bbbk=\mathbb{Q}_p$ then $X,Y,Z\in\mathbb{Z}_p$ with either $Z=1$ or $X=1$, $Z\in p\mathbb{Z}_p$. We can always find such representations by scaling the points.

**Definition 2.4.** For $\Bbbk = \mathbb{Q}$ and $\Bbbk = \mathbb{Q}_p$ define the component maps $\delta_h : C(\Bbbk) \to K_h^*/K_h^{*q}$

$$\delta_h(X,Y,Z) = \begin{cases} (X - \theta_h Z)K_h^{*q} & \text{if } X - \theta_h Z \neq 0, \\ \sqrt[n_h]{\widetilde{F}_h(X,Z)^{-1}K_h^{*q}} & \text{otherwise,} \end{cases}$$

where $\widetilde{F}_h$ is the two-variable polynomial with coefficients in $K_h$ defined by $(X - \theta_h Z)^{n_h}\widetilde{F}_h(X,Z) = F(X,Z)$ and $\sqrt[n_h]{\widetilde{F}_h(X,Z)^{-1}K_h^{*q}}$ is defined to be the unique element $v \in K_h^*/K_h^{*q}$ such that $v^{n_h} = \widetilde{F}_h(X,Z)^{-1}$.

*Remark* 2.5. (1) Note that $v$ exists because the groups $K_h^*/K_h^{*q}$ have exponent $q$ and $\gcd(q, n_h) = 1$ and it is unique since these groups are $\mathbb{F}_q$-vector spaces.

(2) The component maps $\delta_h$ are defined this way because for a point $(X,Y,Z) \in C(\Bbbk)$ with $F(X,Z) \neq 0$, we have that $(X - \theta_h Z)K_h^{*q} \equiv \sqrt[n_h]{\widetilde{F}_h(X,Z)^{-1}K_h^{*q}}$, since $(X - \theta_h Z)^{n_h}\widetilde{F}_h(X,Z) = F(X,Z) = Y^q$.

**Definition 2.6.** Let $\delta_\Bbbk : C(\Bbbk) \to A_\Bbbk^*/A_\Bbbk^{*q}$ be

$$\delta_\Bbbk = (\delta_h)_{h \in \mathcal{F}_\Bbbk}.$$

In order to account for the fact that for any $\lambda \in \Bbbk^*$ and $(X,Y,Z) \in C(\Bbbk)$, $(X,Y,Z) = (\lambda X, \lambda^{n/q} Y, \lambda Z) \in C(\Bbbk)$, we quotient the codomain of $\delta_\Bbbk$ by this action of scalars. So we define an action of $\Bbbk^*$ on $A_\Bbbk^*$ by

$$\lambda\,(\alpha_h)_{h \in \mathcal{F}_\Bbbk} = (\lambda\alpha_h)_{h \in \mathcal{F}_\Bbbk},$$

where $\lambda \in \Bbbk^*$ and $(\alpha_h)_{h \in \mathcal{F}_\Bbbk} \in A_\Bbbk^*$. This action descends to an action of $\Bbbk^*/\Bbbk^{*q}$ on $A_\Bbbk^*/A_\Bbbk^{*q}$. We denote by $A_\Bbbk^*/\Bbbk^* A_\Bbbk^{*q}$ the quotient of $A_\Bbbk^*/A_\Bbbk^{*q}$ by this action.

**Definition 2.7.** Define the ***descent map*** $\mu_\Bbbk$ to be the composition

$$C(\Bbbk) \xrightarrow{\delta_\Bbbk} A_\Bbbk^*/A_\Bbbk^{*q} \xrightarrow{\pi_\Bbbk} A_\Bbbk^*/\Bbbk^* A_\Bbbk^{*q}$$

where $\pi_\Bbbk$ is just the projection to the quotient.

2.2. **The image of $\delta_\mathbb{Q}$.** The image of $\delta_\mathbb{Q}$ is contained in a finite subgroup $A(q, \mathbf{S})$ of $A_\Bbbk^*/A_\Bbbk^{*q}$. To see this let us restrict our attention to finding the allowed possibilities for each of the $\#\mathcal{F}_\mathbb{Q}$ components. Let $h \in \mathcal{F}_\mathbb{Q}$ and set $\widetilde{f}_h(x) = f(x)/(x - \theta_h)^{n_h} \in K_h[x]$.

Suppose $(X,Y,Z) \in C(\mathbb{Q})$ with $X, Y, Z \in \mathbb{Z}$ and $X$ coprime with $Z$. We have that

$$\delta_h(X,Y,Z) = (X - \theta_h Z)K_h^{*q}.$$

Now suppose that $\mathfrak{p} \nmid a_n\mathcal{O}_{K_h}$ is a prime ideal of the ring of integers $\mathcal{O}_{K_h}$ of the number field $K_h$. By assumption we have that

$$\mathrm{ord}_\mathfrak{p}(X - \theta_h Z) \geq 0, \qquad \mathrm{ord}_\mathfrak{p}(\widetilde{F}_h(X,Z)) \geq 0.$$

At this point we want to figure out which primes $\mathfrak{p}$ appear in the factorization of $(X - \theta_h Z)$, but not as a $q$-th power. So suppose $q \nmid \mathrm{ord}_\mathfrak{p}(X - \theta_h Z)$. Since $\gcd(n_h, q) = 1$, this implies that $q \nmid \mathrm{ord}_\mathfrak{p}(\widetilde{F}_h(X,Z))$. In particular we have $X \equiv \theta_h Z$ and $\widetilde{F}_h(X,Z) \equiv 0$ modulo $\mathfrak{p}$, which together give that $\widetilde{F}_h(\theta_h Z, Z) = Z^{n-n_h}\widetilde{f}_h(\theta_h) \equiv 0$ modulo $\mathfrak{p}$. But if $Z \equiv 0$ modulo $\mathfrak{p}$ then also $X \equiv 0$ modulo $\mathfrak{p}$ which contradicts coprimality, so we have that $\mathfrak{p} \in \mathrm{Supp}(\widetilde{f}_h(\theta_h)\mathcal{O}_{K_h})$. By dropping the initial condition on $\mathfrak{p}$ we have that if $q \nmid \mathrm{ord}_\mathfrak{p}(X - \theta_h Z)$ then $\mathfrak{p} \in \mathrm{Supp}(a_n\widetilde{f}_h(\theta_h)\mathcal{O}_{K_h}) \subseteq \mathrm{Supp}(\Delta\mathcal{O}_{K_h})$, where $\Delta = a_n\mathrm{Disc}(g)$. In other words

$$(X - \theta_h Z)\mathcal{O}_{K_h} = \mathfrak{p}_1^{e_1}\ldots\mathfrak{p}_l^{e_l}\mathcal{I}^q$$

where $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_l\} = \mathrm{Supp}\left(a_n\widetilde{f}_h(\theta_h)\mathcal{O}_{K_h}\right)$, $(e_1, \ldots, e_l) \in \mathbb{F}_q^l$ and $\mathcal{I}$ is a fractional ideal of $K_h$.

Now define the sets of primes $S_h = \mathrm{Supp}(a_n\widetilde{f}_h(\theta_h)\mathcal{O}_{K_h})$ for $h \in \mathcal{F}_\mathbb{Q}$. Then by the discussion above $\mathrm{Image}(\delta_h) \subseteq K_h(q, S_h)$ where

$$K_h(q, S_h) := \{\alpha K_h^{*q} : q \mid \mathrm{ord}_\mathfrak{p}(\alpha) \text{ for all } \mathfrak{p} \notin S_h\}.$$

Note that $K_h(q,S_h)$ is a finite subgroup of $K_h^*/K_h^{*q}$ (a proof of this can be found within the proof of Proposition VIII 1.6. in [15]). Therefore we have that

$$\mathrm{Image}(\delta_{\mathbb{Q}}) \subseteq \prod_{h\in\mathcal{F}_{\mathbb{Q}}} K_h(q,S_h) =: A(q,\mathbf{S}) \tag{2.2}$$

which is a finite subgroup of $A_{\mathbb{Q}}^*/A_{\mathbb{Q}}^{*q}$.

2.3. **The image of $\delta_{\Bbbk}$.**

**Definition 2.8.** Define the weighted norm homomorphism $N_{A/\Bbbk} : A_{\Bbbk}^* \to \Bbbk^*$ as

$$N_{A/\Bbbk}\left((\alpha_h)_{h\in\mathcal{F}_{\Bbbk}}\right) = \prod_{h\in\mathcal{F}_{\Bbbk}} N_{K_h/\Bbbk}(\alpha_h)^{n_h}.$$

Since $N_{A/\Bbbk}(A_{\Bbbk}^{*q})$ is a subgroup of $\Bbbk^{*q}$ we also get a homomorphism $\bar{N}_{A/\Bbbk} : A_{\Bbbk}^*/A_{\Bbbk}^{*q} \to \Bbbk^*/\Bbbk^{*q}$.

By commutativity of the following diagram of norm homomorphisms

$$\begin{array}{ccc} A_{\Bbbk}^* & \xrightarrow{N_{A/\Bbbk}} & \Bbbk^* \\ \downarrow & & \downarrow \\ A_{\Bbbk}^*/A_{\Bbbk}^{*q} & \xrightarrow{\bar{N}_{A/\Bbbk}} & \Bbbk^*/\Bbbk^{*q} \end{array}$$

and the fact that

$$N_{A/\Bbbk}\left(\delta_{\Bbbk}(X,Y,Z)\right) = \prod_{h\in\mathcal{F}_{\Bbbk}} N_{K_h/\Bbbk}(X-\theta_h Z)^{n_h} = Z^n \times \prod_{h\in\mathcal{F}_{\Bbbk}} h(X/Z)^{n_h} = \frac{Y^q}{a_n}$$

we can deduce that

$$\mathrm{Image}(\delta_{\Bbbk}) \subseteq \bar{N}_{A/\Bbbk}^{-1}\left(\frac{1}{a_n}\Bbbk^{*q}\right) =: H_{\Bbbk}$$

which, if non-empty, is a coset of the subgroup $\mathrm{Kernel}(\bar{N}_{A/\Bbbk})$ in $A_{\Bbbk}^*/A_{\Bbbk}^{*q}$. Combining this with the inclusion (2.2) we deduce that

$$\mathrm{Image}(\delta_{\mathbb{Q}}) \subseteq H_{\mathbb{Q}} \cap A(q,\mathbf{S}) =: H_{\mathbb{Q}}(\mathbf{S}).$$

2.4. **The image of $\mu_{\mathbb{Q}}$.**

**Lemma 2.9.** *Let $A_{\mathbb{Q}}$ be the semi-simple $\mathbb{Q}$-algebra associated to the curve $C$ and $A(q,\mathbf{S})$ be the subgroup of $A_{\mathbb{Q}}^*/A_{\mathbb{Q}}^{*q}$ defined in* (2.2)*. Also set*

$$T := \{p \text{ prime} : \text{for all } h\in\mathcal{F}_{\mathbb{Q}}, \text{ and all } \mathfrak{p}\in\mathrm{Supp}(p\mathcal{O}_{K_h}), (q \mid \mathrm{ord}_{\mathfrak{p}}(p\mathcal{O}_{K_h})) \text{ or } (\mathfrak{p}\in S_h)\}.$$

$$\begin{array}{ccccccc} \mathbb{Q}^*/\mathbb{Q}^{*q} & \xrightarrow{\iota} & A_{\mathbb{Q}}^*/A_{\mathbb{Q}}^{*q} & \xrightarrow{\pi_{\mathbb{Q}}} & A_{\mathbb{Q}}^*/\mathbb{Q}^*A_{\mathbb{Q}}^{*q} & \longrightarrow & 1 \\ \uparrow & & \uparrow & \nearrow & & & \\ \mathbb{Q}(q,T) & & A(q,\mathbf{S}) & & & & \end{array}$$

*Then*

*(i)* $\mathrm{Image}(\iota) \cap A(q,\mathbf{S}) = \iota\left(\mathbb{Q}(q,T)\right)$

*(ii)* $\pi_{\mathbb{Q}}\left(A(q,\mathbf{S})\right) \cong A(q,\mathbf{S})/\iota\left(\mathbb{Q}(q,T)\right)$.

*Proof.* (i) First suppose that $aA^{*q} \in \iota\left(\mathbb{Q}(q,T)\right)$. Then $q \mid \mathrm{ord}_p(a)$ for all $p \notin T$. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_{K_h}$ for some $h$, with $\mathfrak{p}\notin S_h$. We know that

$$\mathrm{ord}_{\mathfrak{p}}(a\mathcal{O}_{K_h}) = \mathrm{ord}_{\mathfrak{p}}(p\mathcal{O}_{K_h}) \times \mathrm{ord}_p(a)$$

so by the definition of $T$ at least one of the factors will be divisible by $q$ thus also their product, which implies that $aA^{*q} \in A(q,\mathbf{S})$.

For the opposite inclusion, suppose that $a\in\mathbb{Q}^*$ and $aA^{*q}\in A(q,\mathbf{S})$. Then $q \mid \mathrm{ord}_{\mathfrak{p}}(a\mathcal{O}_{K_h})$ for all

$h \in \mathcal{F}_{\mathbb{Q}}$ and for all $\mathfrak{p} \notin S_h$ so if $p \notin T$, then $q$ must divide $\mathrm{ord}_p(a)$ since $q$ divides the product but not the first factor in the equality above.

(ii) We have

$$\pi_{\mathbb{Q}}\left(A(q,\mathbf{S})\right) \cong \frac{A(q,\mathbf{S})}{\mathrm{Kernel}(\pi_{\mathbb{Q}}) \cap A(q,\mathbf{S})} = \frac{A(q,\mathbf{S})}{\mathrm{Image}(\iota) \cap A(q,\mathbf{S})} \overset{(i)}{=} \frac{A(q,\mathbf{S})}{\iota\left(\mathbb{Q}(q,T)\right)}$$

□

Let us denote $\pi_{\mathbb{Q}}(H_{\mathbb{Q}}(\mathbf{S}))$ by $\bar{H}_{\mathbb{Q}}(\mathbf{S})$. Since $\mathrm{Image}(\delta_{\mathbb{Q}}) \subseteq H_{\mathbb{Q}}(\mathbf{S})$, we have that

$$\mathrm{Image}(\mu_{\mathbb{Q}}) \subseteq \bar{H}_{\mathbb{Q}}(\mathbf{S}). \tag{2.3}$$

In the following section we will see how $\mathrm{Image}(\mu_{\mathbb{Q}})$ is contained in a potentially strict subset of $\bar{H}_{\mathbb{Q}}(\mathbf{S})$ and provide an algorithm to compute it.

## 3. The Selmer set

3.1. **Determining the image of $\mu_{\mathbb{Q}_p}$.** In this section we will provide an algorithm which determines $\mathrm{Image}(\mu_{\mathbb{Q}_p})$ for a rational prime $p$. The algorithm relies on the fact that points of $C$ which lie in a "sufficiently small" $p$-adic neighborhood, have the same image under $\mu_{\mathbb{Q}_p}$.

The diagram below is crucial in the process of refining the possible image of $\mu$ even further:

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\mu_{\mathbb{Q}}} & A_{\mathbb{Q}}^*/\mathbb{Q}^* A_{\mathbb{Q}}^{*q} \\ \downarrow{\scriptstyle \iota_p} & & \downarrow{\scriptstyle r_p} \\ C(\mathbb{Q}_p) & \xrightarrow{\mu_{\mathbb{Q}_p}} & A_{\mathbb{Q}_p}^*/\mathbb{Q}_p^* A_{\mathbb{Q}_p}^{*q} \end{array}$$

By commutativity, if we have a rational point $P \in C(\mathbb{Q})$ then $\mu_{\mathbb{Q}_p} \circ \iota_p(P) = r_p \circ \mu_{\mathbb{Q}}(P)$. Therefore we have that

$$\mathrm{Image}(\mu_{\mathbb{Q}}) \subseteq r_p^{-1}(\mathrm{Image}(\mu_{\mathbb{Q}_p})) \cap \bar{H}_{\mathbb{Q}}(\mathbf{S}) \tag{3.1}$$

**Definition 3.1.** The **Selmer set** over $\mathbb{Q}$ of the superelliptic curve $C$, is defined as

$$\mathrm{Sel}^{(\mu)}(C,\mathbb{Q}) = \left\{[\alpha] \in \bar{H}_{\mathbb{Q}}(\mathbf{S}) : r_p([\alpha]) \in \mathrm{Image}(\mu_{\mathbb{Q}_p}) \text{ for all rational primes } p\right\}.$$

*Remark* 3.2. Strictly speaking, the set defined here corresponds to the "fake " Selmer set found generally in the literature (e.g. [6] and [7]). Roughly, the difference between the fake and the actual Selmer set is that the latter distinguishes between covers (defined in Section 3.2) $\phi_\alpha : D_\alpha \to C$ and $\phi_{\alpha'} : D_{\alpha'} \to C$ when $\phi_\alpha$ and $\phi_{\alpha'}$ are different even if $D_\alpha$ and $D_{\alpha'}$ are isomorphic. Since we are not using both sets, we omit the "fake" from the notation.

After considering the inclusion (2.3) in the end of Section 2.4 and the inclusions (3.1) for every rational prime $p$ we get that

$$\mathrm{Image}(\mu_{\mathbb{Q}}) \subseteq \mathrm{Sel}^{(\mu)}(C,\mathbb{Q}).$$

Let $h \in \mathcal{F}_{\mathbb{Q}_p}$ and denote by $\mathfrak{p}_h$ the prime of $\mathcal{O}_{K_h}$. The following two lemmas are used to show that the analytic space $C(\mathbb{Q}_p)$ can be covered by a finite number of neighborhoods, where the map $\mu_{\mathbb{Q}_p}$ is constant. In practice $X_k$ (or $X$) will be a finite precision approximation to the first coordinate of a point $(X',Y',1) \in C(\mathbb{Q}_p)$.

**Lemma 3.3.** *Suppose that $X', X_k \in \mathbb{Z}_p$ with $\mathrm{ord}_p(X' - X_k) \geq k$*

*(i) If $k \geq \frac{2\,\mathrm{ord}_{\mathfrak{p}_h}(q) + \mathrm{ord}_{\mathfrak{p}_h}(X_k - \theta_h) + 1}{e_{\mathfrak{p}_h/p}}$ then $(X_k - \theta_h)K_h^{*q} = (X' - \theta_h)K_h^{*q}$.*

*(ii) If $k \geq \frac{2\,\mathrm{ord}_{\mathfrak{p}_h}(q) + \mathrm{ord}_{\mathfrak{p}_h}(\widetilde{f}_h(X_k)) + 1}{e_{\mathfrak{p}_h/p}}$ then $\widetilde{f}_h(X_k)K_h^{*q} = \widetilde{f}_h(X')K_h^{*q}$.*

*Proof.* (i) By the assumption $X' = X_k + up^k$ where $u \in \mathbb{Z}_p$. So

$$\frac{X' - \theta_h}{X_k - \theta_h} = 1 + \frac{up^k}{X_k - \theta_h}.$$

Now let $\tau(t) = \frac{X'-\theta_h}{X_k-\theta_h} - t^q$. By Hensel's lemma we have that the following is a sufficient condition for $\tau$ to have a solution in $K_h$,

$$\operatorname{ord}_{\mathfrak{p}_h}(\tau(1)) \geq 2\operatorname{ord}_{\mathfrak{p}_h}\left(\frac{d\tau}{dt}(1)\right) + 1$$

$$k\operatorname{ord}_{\mathfrak{p}_h}(p) - \operatorname{ord}_{\mathfrak{p}_h}(X_k - \theta_h) \geq 2\operatorname{ord}_{\mathfrak{p}_h}(q) + 1$$

So as long as the condition of the lemma is satisfied Hensel's lemma ensures that $(X_k - \theta_h)$ and $(X' - \theta_h)$ are the same modulo $K_h^{*q}$.

(ii) This is very similar to the previous part. Just use the fact that $\widetilde{f}_h(X') = \widetilde{f}_h(X_k + up^k) = \widetilde{f}_h(X_k) + vp^k$ where $v \in \mathbb{Z}_p$ and set $\tau(t) = \frac{\widetilde{f}_h(X')}{\widetilde{f}_h(X_k)} - t^q$.

□

**Lemma 3.4.** *If $\{X_k\}_{k=1}^{\infty} \subset \mathbb{Z}_p$ is a sequence satisfying $\operatorname{ord}_p(X' - X_k) \geq k$ for some $X' \in \mathbb{Z}_p$ and every $k$, then there exists $N \in \mathbb{Z}_{>0}$ such that $X_N$ satisfies at least one of conditions (i) or (ii) of Lemma 3.3.*

*Proof.* Suppose such $N$ does not exist. This means that for every $k$ we have

$$\min\left\{\frac{2\operatorname{ord}_{\mathfrak{p}_h}(q) + \operatorname{ord}_{\mathfrak{p}_h}(X_k - \theta_h) + 1}{e_{\mathfrak{p}_h/p}}, \frac{2\operatorname{ord}_{\mathfrak{p}_h}(q) + \operatorname{ord}_{\mathfrak{p}_h}(\widetilde{f}_h(X_k)) + 1}{e_{\mathfrak{p}_h/p}}\right\} > k$$

and therefore both $\operatorname{ord}_{\mathfrak{p}_h}(X_k - \theta_h)$ and $\operatorname{ord}_{\mathfrak{p}_h}(\widetilde{f}_h(X_k))$ tend to infinity as $k$ tends to infinity. But since $\{X_k\}_{k=1}^{\infty}$ converges to $X'$ we have that $(X' - \theta_h) = \widetilde{f}_h(X') = 0$, a contradiction. □

A clear distinction between the case of hyperelliptic ($q = 2$) and superelliptic ($q > 2$) curves is that, a superelliptic curve is allowed to have singularities, since $f$ being $q$-th power-free is no longer equivalent to $f$ not having repeated roots. At this point we would like to use some version of Hensel's Lemma to determine whether our finite precision $X_k$ lifts to $\mathbb{Z}_p$ as the first coordinate of a point $(X', Y', 1) \in C(\mathbb{Q}_p)$. We have to be careful not to ask this question for points approximating one of the singularities as that would result in an infinite loop. Thus we have to determine the size of the $\mu_{\mathbb{Q}_p}$-constant neighborhood around each singularity (which is defined over $\mathbb{Q}_p$) in advance and compute its image.

Let

$$\mathcal{F}_{\mathbb{Q}_p}^{lsi} = \left\{h \in \mathcal{F}_{\mathbb{Q}_p} : \deg(h) = 1, n_h > 1, \theta_h \in \mathbb{Z}_p\right\},$$

where the exponent $lsi$ stands for linear,singular and integral. Elements of this set correspond to the singular points on $C$ that are defined over $\mathbb{Q}_p$, but are of the form $(\theta_h, 0, 1)$ with $\theta_h \in \mathbb{Z}_p$. The last condition arises because we split the computation into two parts, the first being the determination of the image under $\mu_{\mathbb{Q}_p}$ of points of the form $(X', Y', 1) \in C(\mathbb{Q}_p)$, with $X', Y' \in \mathbb{Z}_p$.

Consider the following functions:

**function** SizeOfNeighborhood($h$)
  $k_h \leftarrow 0$
  Finish $\leftarrow$ **false**
  **while** [ Finish = **false**] **do**
    $k_h \leftarrow k_h + 1$
    $X \leftarrow X \in \mathbb{Z} \subset \mathbb{Z}_p : \operatorname{ord}_{\mathfrak{p}_h}(X - \theta_h) \geq k_h$
    ValList$\leftarrow \left\{\frac{2\operatorname{ord}_{\mathfrak{p}_{h'}}(q) + \operatorname{ord}_{\mathfrak{p}_{h'}}(X - \theta_{h'}) + 1}{e_{\mathfrak{p}_{h'}/p}} : h' \in \mathcal{F}_{\mathbb{Q}_p} \setminus \{h\}\right\} \cup \left\{2\operatorname{ord}_{\mathfrak{p}_h}(q) + \operatorname{ord}_{\mathfrak{p}_h}(\widetilde{f}_h(X)) + 1\right\}$
    **if** [ max(ValList) $\leq k_h$ ] **then**
      Finish $\leftarrow$ **true**

10: **end if**
11: **end while**
12: **return** $k_h, X$
13: **end function**

Note that the function SIZEOFNEIGHBORHOOD only makes sense when $\deg(h) = 1$ otherwise we would not be able to find an $X$ satisfying the condition of step 6 for every given $k_h$ (that would imply that $\theta_h \in \mathbb{Z}_p$), and we will actually only apply it to elements of $\mathcal{F}^{lsi}_{\mathbb{Q}_p}$. This function has a double use: The returned value of $X$ will be used to compute $\mu_{\mathbb{Q}_p}(\theta_h, 0, 1)$, and $k_h$ will keep track of the size of the $\mu_{\mathbb{Q}_p}$-constant neighborhood around the singularity. Now for $h \in \mathcal{F}^{lsi}_{\mathbb{Q}_p}$ set

$$\mathcal{U}_h = \{X \in \mathbb{Z}_p : \mathrm{ord}_p(X - \theta_h) \geq k_h\}$$

and

$$\mathcal{U} = \bigcup_{h \in \mathcal{F}^{lsi}_{\mathbb{Q}_p}} \mathcal{U}_h.$$

The following function can be thought of as partitioning $\mathbb{Z}_p$ into neighborhoods, with the partition becoming finer close to the singularities. Then the function LOCALIMAGE will test each of these neighborhoods for elements that lift to points on $C$, and if necessary partition them further into $\mu_{\mathbb{Q}_p}$-constant parts.

**function** COMPUTEINPUTLIST(REPS, $k$, LIST)
  **for** $X \in$ REPS **do**
    **if** [ $\exists h \in \mathcal{F}^{lsi}_{\mathbb{Q}_p}$ : [ $k_h > k$ **and** $\mathrm{ord}_p(X - \theta_h) \geq k_h$ ] ] **then**
      LIST $\leftarrow$COMPUTEINPUTLIST$\big(\{X + tp^k : t \in \{0, \ldots, p-1\}\}, k+1,$ LIST$\big)$
    **else**
      LIST $\leftarrow$ LIST $\cup\{(X, k)\}$
    **end if**
  **end for**
  **return** LIST
**end function**

At this point we should stress that the functions SIZEOFNEIGHBORHOOD and COMPUTEINPUTLIST would be redundant if there were no singularities, and the function LOCALIMAGE would be sufficient to compute the local image. In that case the input (LIST$=\{0, \ldots, p-1\}$,IMAGE$=\{\}$) would produce the require result.

**function** LOCALIMAGE(LIST, IMAGE)
  **for** [ $(X, k) \in$ LIST ] **do**
    **if** [ $X \in \mathcal{U}$ **or** $\nexists (X', Y', 1) \in C(\mathbb{Q}_p) : \mathrm{ord}_p(X' - X) \geq k$ ] **then**
      LIST $\leftarrow$ LIST$\setminus\{(X, k)\}$
    **else**
      VALLIST$\leftarrow \left\{ \left[ \frac{2\,\mathrm{ord}_{\mathfrak{p}_h}(q) + \mathrm{ord}_{\mathfrak{p}_h}(X - \theta_h) + 1}{e_{\mathfrak{p}_h/p}}, \frac{2\,\mathrm{ord}_{\mathfrak{p}_h}(q) + \mathrm{ord}_{\mathfrak{p}_h}(\widetilde{f}_h(X)) + 1}{e_{\mathfrak{p}_h/p}} \right] : h \in \mathcal{F}_{\mathbb{Q}_p} \right\}$
      **if** [ $\forall [k_1, k_2] \in$VALLIST $\min(k_1, k_2) \leq k$ ] **then**
        NEWELEMENT $\leftarrow 1$
        **for** [ $[k_1, k_2] \in$VALLIST ] **do**
          **if** [ $k_1 \leq k_2$ ] **then**
            NEWELEMENT $\leftarrow$ NEWELEMENT$\times (X - \theta_h) K_h^{*q}$
          **else**
            NEWELEMENT$\leftarrow$ NEWELEMENT $\times \sqrt[n_h]{\widetilde{f}_h(X)^{-1} K_h^{*q}}$
          **end if**
        **end for**
        NEWELEMENT$\leftarrow$ $\pi_{\mathbb{Q}_p}$ (NEWELEMENT)

```
17:             IMAGE ← IMAGE ∪{NEWELEMENT}
18:         else
19:             NEWLIST← {(X + tp^k, k + 1) : t ∈ {0, . . . , p − 1}}
20:             IMAGE←LOCALIMAGE(NEWLIST, IMAGE)
21:         end if
22:     end if
23:   end for
24:   return IMAGE
25: end function
```

With the help of the SIZEOFNEIGHBORHOOD function, we pre-compute and store in the variable *image* the images of the singular points under $\mu_{\mathbb{Q}_p}$. Using LOCALIMAGE with initial input

$$(\text{COMPUTEINPUTLIST}\left(\{0,\dots,p-1\},1,\{\}\right),\text{image})$$

we get as output a set $V_1 \subseteq A^*_{\mathbb{Q}_p}/\mathbb{Q}_p^* A^{*q}_{\mathbb{Q}_p}$ which satisfies $\mu_{\mathbb{Q}_p}(U_1) = V_1$, where $U_1 = \{(X, Y, 1) \in C(\mathbb{Q}_p) : X, Y \in \mathbb{Z}_p\}$. With slight modifications to the routine above we can also obtain as output a set $V_2$ such that $\mu_{\mathbb{Q}_p}(U_2) = V_2$, where $U_2 = \{(1, Y, pZ) \in C(\mathbb{Q}_p) : Y, Z \in \mathbb{Z}_p\}$. Thus we obtain the complete image of $\mu_{\mathbb{Q}_p}$, since $U_1 \cup U_2 = C(\mathbb{Q}_p)$.

*Remark* 3.5. We can be certain that the routine LocalImage terminates after a finite number of steps because of Lemma 3.4. An infinite loop would correspond to a sequence $\{X_k\}_{k=1}^{\infty}$ converging to some $X' \in \mathbb{Z}_p$ satisfying $X' - \theta_h = \widetilde{f}_h(X') = 0$ which is impossible. Also note that the If statement at step 3, ensures that if $X \in \mathcal{U}$, in other words if our approximate value is very close to the first coordinate of one of the singular points, then it is excluded from LIST and we do not try to lift it using Hensel's Lemma, which would have resulted in an infinite loop.

3.2. **The corresponding covers.** For every $\alpha \in A^*_{\Bbbk}$ such that $[\alpha] := \alpha\mathbb{Q}^* A^{*q} \in \bar{H}_{\Bbbk}$ we can construct an unramified cover of $C$ of degree $q^{d-2}$

$$\phi_\alpha : D_\alpha \to C,$$

defined over $\Bbbk$ satisfying the properties

$$\begin{aligned} D_\alpha(\Bbbk) \neq \emptyset \quad &\Leftrightarrow \quad [\alpha] \in \text{Image}(\mu_{\Bbbk}) \\ [\alpha] = [\alpha'] \quad &\Rightarrow \quad D_\alpha \cong D_{\alpha'} \end{aligned}$$

First let us give an equivalent description of the $\Bbbk$-algebra $A_{\Bbbk}$. Denote the absolute Galois group $\text{Gal}(\bar{\Bbbk}/\Bbbk)$ by $\mathcal{G}_{\Bbbk}$. We fix embeddings $K_h \hookrightarrow \bar{\Bbbk}$ for all $h \in \mathcal{F}_{\Bbbk}$ that are compatible in the sense that they agree on the intersections $K_h \cap K_{h'}$ for $h, h' \in \mathcal{F}_{\Bbbk}$. We then get an inclusion $\Theta_{\Bbbk} \hookrightarrow \Theta_{\bar{\Bbbk}}$ and we can treat elements $\alpha_h \in K_h$ as elements of $\bar{\Bbbk}$ and elements of $\Theta_{\Bbbk}$ as elements of $\Theta_{\bar{\Bbbk}}$.

**Lemma 3.6.**

$$A_{\Bbbk} \cong \text{Map}_{\Bbbk}(\Theta_{\bar{\Bbbk}}, \bar{\Bbbk}),$$

*where the right hand side is the set of all $\mathcal{G}_{\Bbbk}$-equivariant maps from $\Theta_{\bar{\Bbbk}}$ to $\bar{\Bbbk}$.*

*Proof.* The isomorphism is given by

$$(\alpha_h)_{h\in\mathcal{F}_{\Bbbk}} \mapsto (\theta_{h'} \mapsto {}^{\sigma}\alpha_h : \sigma \in \mathcal{G}_{\Bbbk},\ h \in \mathcal{F}_{\Bbbk},\ {}^{\sigma}\theta_h = \theta_{h'})$$

with inverse

$$\xi \mapsto (\xi(\theta_h))_{\theta_h \in \Theta_{\Bbbk} \subseteq \Theta_{\bar{\Bbbk}}}.$$

$\square$

Let $\alpha \in A_{\mathbb{k}}^*$ such that $[\alpha] \in \bar{H}_{\mathbb{k}}$. Since $\alpha A^{*q} \in H_{\mathbb{k}}$, there exists $v \in \mathbb{k}^*$ with $a_n N_{A/\mathbb{k}}(\alpha) = v^q$. Let $D_\alpha$ be the variety in $\mathbb{P}^{d-1} \times C$ defined by

$$\begin{aligned} \big((u_h)_{h\in\mathcal{F}_{\bar{\mathbb{k}}}}, (X,Y,Z)\big) \in D_\alpha \Leftrightarrow & \exists\lambda \neq 0 \text{ s.t. } \lambda\alpha(\theta_h)u_h^q = X - \theta_h Z \\ & \text{for all } h \in \mathcal{F}_{\bar{\mathbb{k}}} \text{ and} \\ & \lambda^{n/q} v \prod_{h\in\mathcal{F}_{\bar{\mathbb{k}}}} u_h^{n_h} = Y \end{aligned} \tag{3.2}$$

We use a description of the covers $D_\alpha$ similar, at least in terms of their ambient space, to the one found in [7] and [14]. We equip the first factor, $\mathbb{P}^{d-1}$, with the twisted $\mathcal{G}_{\mathbb{k}}$-action which permutes coordinates in the same way it permutes $\Theta_{\bar{\mathbb{k}}}$. In other words if $\sigma \in \mathcal{G}_{\mathbb{k}}$ satisfies ${}^\sigma\theta_h = \theta_{h'}$, then ${}^\sigma u_h = u_{h'}$. It is then obvious from the definition that $D_\alpha$ is actually defined over $\mathbb{k}$. Projection to the second factor gives rise to the required covering map

$$\phi_\alpha : D_\alpha \to C.$$

**Lemma 3.7.** *The map $\phi_\alpha : D_\alpha \to C$ is unramified of degree $q^{d-2}$. In particular $D_\alpha$ is a curve.*

*Proof.* Let $(X,Y,Z) \in C(\bar{\mathbb{k}})$ and suppose $X - \theta_{h_0}Z \neq 0$ for some $h_0 \in \mathcal{F}_{\bar{\mathbb{k}}}$. Then $u_{h_0} \neq 0$ so we can set $u_{h_0} = 1$. By doing this we also fixed $\lambda = \frac{X-\theta_{h_0}Z}{\alpha(\theta_{h_0})}$. So for all $u_h$ with $h \neq h_0$ we have

$$u_h^q = \frac{\alpha(\theta_{h_0})(X-\theta_h Z)}{\alpha(\theta_h)(X-\theta_{h_0}Z)}.$$

Since we are over $\bar{\mathbb{k}}$, if there does not exist $h \in \mathcal{F}_{\bar{\mathbb{k}}}$ such that $X - \theta_h Z = 0$, then there are exactly $q$ different choices for the value of each of the $d-1$ $u_h$'s. Once $d-2$ of them have been chosen, the remaining one is decided by the relation

$$\lambda^{n/q} v \prod_{h\in\mathcal{F}_{\bar{\mathbb{k}}}} u_h^{n_h} = Y.$$

The fact that there is a unique choice for the value of the remaining coordinate uses that $\gcd(n_h, q) = 1$ for every $h \in \mathcal{F}_{\bar{\mathbb{k}}}$. On the other hand if $X - \theta_{h'}Z = 0$ for some $h' \in \mathcal{F}_{\bar{\mathbb{k}}} \setminus \{h_0\}$ then $u_{h'} = 0$ and there are $q$ choices for the remaining $d-2$ $u_h$'s. The extra relation in this case does not decide the value for any of them. We see that in both cases the fiber of $\phi_\alpha$ over $P \in C(\bar{\mathbb{k}})$ contains exactly $q^{d-2}$ points. $\square$

**Proposition 3.8.** *$D_\alpha(\mathbb{k}) \neq \emptyset$ if and only if $[\alpha] \in \mathrm{Image}(\mu_{\mathbb{k}})$. Furthermore, if $[\alpha] = [\alpha']$ then $D_\alpha \cong D_{\alpha'}$ over $\mathbb{k}$. In other words, up to $\mathbb{k}$-isomorphism, $D_\alpha$ only depends on the class $[\alpha]$ in $A_{\mathbb{k}}^*/\mathbb{k}^* A_{\mathbb{k}}^{*q}$.*

*Proof.* Let $P = \big((u_h)_{h\in\mathcal{F}_{\bar{\mathbb{k}}}}, (X,Y,Z)\big) \in D_\alpha(\mathbb{k})$. Projecting gives $\phi_\alpha(P) = (X,Y,Z) \in C(\mathbb{k})$ and if $X - \theta_h Z \neq 0 \ \forall\ h \in \mathcal{F}_{\bar{\mathbb{k}}}$ then

$$\delta_{\mathbb{k}}\left(\phi_\alpha(P)\right) = \big((X-\theta_h Z)K_h^{*q}\big)_{\theta_h\in\Theta_{\mathbb{k}}\subseteq\Theta_{\bar{\mathbb{k}}}} = \big(\lambda\alpha_h u_h^q K_h^{*q}\big)_{\theta_h\in\Theta_{\mathbb{k}}\subseteq\Theta_{\bar{\mathbb{k}}}}$$

therefore $\mu_{\Bbbk}(\phi_\alpha(P)) = [\alpha]$. On the other hand if there exists $h' \in \mathcal{F}_{\bar{\Bbbk}}$ such that $X - \theta_{h'} Z = 0$ then by definition of $\delta_{h'}$ we have

$$\begin{aligned}
\delta_{h'}(\phi_\alpha(P)) &= \sqrt[n_{h'}]{\widetilde{F}_{h'}(X,Z)^{-1} K_{h'}^{*q}} \\
&= \sqrt[n_{h'}]{\frac{1}{a_n \prod\limits_{h \in \mathcal{F}_{\bar{\Bbbk}} \setminus h'} (X - \theta_h Z)^{n_h}} K_{h'}^{*q}} \\
&= \sqrt[n_{h'}]{\frac{1}{a_n \lambda^{n - n_{h'}} \prod\limits_{h \in \mathcal{F}_{\bar{\Bbbk}} \setminus h'} \left(\alpha(\theta_h) u_h^q\right)^{n_h}} K_{h'}^{*q}} \\
&= \sqrt[n_{h'}]{\frac{(\lambda \alpha_{h'})^{n_{h'}}}{a_n \lambda^n N_{A/\Bbbk}(\alpha)} K_{h'}^{*q}} \\
&= \sqrt[n_{h'}]{\frac{(\lambda \alpha_{h'})^{n_{h'}}}{\left(\lambda^{n/q} v\right)^q} K_{h'}^{*q}} \\
&= \sqrt[n_{h'}]{(\lambda \alpha_{h'})^{n_{h'}} K_{h'}^{*q}} \\
&= \lambda \alpha_{h'} K_{h'}^{*q}.
\end{aligned}$$

So again $\mu_{\Bbbk}(\phi_\alpha(P)) = [\alpha]$, since all the other components of $\delta_{\Bbbk}$ are evaluated without using cofactors.

For the other implication, suppose $[\alpha] \in \operatorname{Image}(\mu_{\Bbbk})$. This means there exist $X, Y, Z \in \mathcal{O}_{\Bbbk}$, $\lambda \in \Bbbk^*$ and $\beta \in A_{\Bbbk}^*$ such that

$$\lambda \alpha(\theta_h) \beta(\theta_h)^q = X - \theta_h Z$$

for $\theta_h \in \Theta_{\Bbbk}$. After conjugating these relations by elements of $\mathcal{G}_{\Bbbk}$ and using the fact that $\alpha$ and $\beta$ are $\mathcal{G}_{\Bbbk}$-equivariant, we obtain the corresponding relations for $\theta_h \in \Theta_{\bar{\Bbbk}} \setminus \Theta_{\Bbbk}$. Then $\left((\beta(\theta_h))_{h \in \mathcal{F}_{\bar{\Bbbk}}}, (X,Y,Z)\right) \in D_\alpha(\Bbbk)$. Note that if for some $h' \in \mathcal{F}_{\Bbbk}$ we have $X - \theta_{h'} Z = 0$ then $d_{h'} = 1$ and the corresponding coordinate $u_{h'}$ is equal to zero.

For the last statement suppose that we have $\alpha, \alpha' \in A_{\Bbbk}^*$ with $[\alpha] = [\alpha']$. This implies that there exist $\lambda \in \Bbbk^*$ and $\beta \in A_{\Bbbk}^*$ such that $\alpha = \lambda \alpha' \beta^q$. By definition of the covers it is not hard to see that we can then map $D_\alpha$ to $D_{\alpha'}$ via $\left((u_h)_{h \in \mathcal{F}_{\bar{\Bbbk}}}, (X,Y,Z)\right) \mapsto \left((\beta(\theta_h) u_h)_{h \in \mathcal{F}_{\bar{\Bbbk}}}, (X,Y,Z)\right)$ which is clearly an isomorphism and it is defined over $\Bbbk$ since it is invariant under the twisted $\mathcal{G}_{\Bbbk}$-action. □

**Corollary 3.9.** *Let $\mathcal{H}$ be any subset of $\bar{H}_{\mathbb{Q}}(\mathbf{S})$ containing* $\operatorname{Image}(\mu_{\mathbb{Q}})$*, then*

$$C(\mathbb{Q}) = \bigcup_{[\alpha] \in \mathcal{H}} \phi_\alpha\left(D_\alpha(\mathbb{Q})\right).$$

*In particular the above equality holds for $\mathcal{H} = \operatorname{Sel}^{(\mu)}(C, \mathbb{Q})$.*

*Proof.* Since for all $\alpha \in A_{\mathbb{Q}}^*$ such that $[\alpha] \in \bar{H}_{\mathbb{Q}}$, $D_\alpha$ and $\phi_\alpha$ are defined over $\mathbb{Q}$, we know that the right hand side is contained in $C(\mathbb{Q})$. Also, from the proof of Proposition 3.8 we deduce that if we have $P \in C(\mathbb{Q})$ and $\mu_{\mathbb{Q}}(P) = [\alpha]$ then there exists $Q \in D_\alpha(\mathbb{Q})$ with $\phi_\alpha(Q) = P$. On the other hand, if $[\alpha] \in \mathcal{H} \setminus \operatorname{Image}(\mu_{\mathbb{Q}})$ then $D_\alpha(\mathbb{Q}) = \emptyset$. □

**Proposition 3.10.** *The curves $D_\alpha$ are non-singular.*

*Proof.* To show this let us restrict to the affine patch where $u_{h_0} \neq 0$ and $Z \neq 0$ for some $h_0 \in \mathcal{F}_{\bar{\Bbbk}}$. We thus assume that $u_{h_0} = Z = 1$, label the elements of $\mathcal{F}_{\bar{\Bbbk}} \setminus \{h_0\}$ using an index $i \in \{1, \ldots, d-1\}$ and rename $u_i := u_{h_i}$, $\theta_i := \theta_{h_i}$ and $n_i := n_{h_i}$ to simplify the notation. The defining equations for $D_\alpha$ in

this patch become

$$\begin{aligned}\alpha(\theta_i)(X-\theta_0)u_i^q =&\alpha(\theta_0)(X-\theta_i) \qquad \text{for } i\in\{1,\dots,d-1\}\\ v(X-\theta_0)^{n/q}\prod_{i=1}^{d-1}u_i^{n_i} =&Y.\end{aligned}$$

We get the following $(d+1)\times d$ matrix of partial derivatives which represents a linear map whose cokernel is the cotangent space of $D_\alpha$ at a generic point of the affine patch.

$$\begin{pmatrix} \alpha(\theta_1)u_1^q-\alpha(\theta_0) & \alpha(\theta_2)u_2^q-\alpha(\theta_0) & \dots & \alpha(\theta_{d-1})u_{d-1}^q-\alpha(\theta_0) & v\left(\frac{n}{q}\right)(X-\theta_0)^{n/q-1}\prod_{i=1}^{d-1}u_i^{n_i}\\ q\alpha(\theta_1)(X-\theta_0)u_1^{q-1} & 0 & \dots & 0 & vn_1(X-\theta_0)^{n/q}u_1^{n_1-1}\prod_{i\neq 0,1}u_i^{n_i}\\ 0 & q\alpha(\theta_2)(X-\theta_0)u_2^{q-1} & \dots & 0 & vn_2(X-\theta_0)^{n/q}u_2^{n_2-1}\prod_{i\neq 0,2}u_i^{n_i}\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & \dots & q\alpha(\theta_{d-1})(X-\theta_0)u_{d-1}^{q-1} & vn_{d-1}(X-\theta_0)^{n/q}u_{d-1}^{n_{d-1}-1}\prod_{i\neq 0,d-1}u_i^{n_i}\\ 0 & 0 & \dots & 0 & -1\end{pmatrix} \tag{3.3}$$

This matrix has rank $d$ at every point of the affine patch. To see this note that the first $d-1$ entries of the first row, can never be zero, since this would contradict the fact that the roots of $g$ are distinct. For the same reason, at most one row can be identically zero and when this happens the $d\times d$ matrix obtained by deleting that row has rank $d$. A similar argument for all of the $2d$ affine patches covering $D_\alpha$ shows that $D_\alpha$ is non-singular. ☐

**Proposition 3.11.** *If $p$ is a rational prime such that $p\nmid q\Delta$ and $\alpha\in A^*_{\mathbb{Q}}$ such that $[\alpha]\in \bar{H}_{\mathbb{Q}}(\mathbf{S})$, then $D_\beta$ has good reduction, where $\beta\in A^*_{\mathbb{Q}_p}$ is such that $[\beta]=r_p([\alpha])$.*

*Proof.* Since $p$ does not divide $q$ or the discriminant of $g$, $\alpha\in A^*_{\mathbb{Q}}$ can be chosen such that $\operatorname{ord}_{\mathfrak{p}}(\alpha(\theta_h))=0$ for every $h\in\mathcal{F}_{\bar{\mathbb{Q}}}$ and every $\mathfrak{p}\mid p$. Take $\beta$ to be the image of this $\alpha$ under the inclusion $\otimes\mathbb{Q}_p : A^*_{\mathbb{Q}}\to A^*_{\mathbb{Q}_p}$. Then $[\beta]=r_p([\alpha])$ and also $\operatorname{ord}_{\mathfrak{p}}(\beta(\theta_h))=0$ for every $h\in\mathcal{F}_{\bar{\mathbb{Q}}_p}$ and every $\mathfrak{p}\mid p$. Thus the defining equation

$$\lambda\beta(\theta_h)u_h^q = X-\theta_h Z$$

of $D_\beta$ can be reduced to an equation modulo $\mathfrak{p}_h$ for every $h\in\mathcal{F}_{\bar{\mathbb{Q}}_p}$, where $\mathfrak{p}_h$ is the prime of $K_h$ above $p$. We thus get an unramified cover $\overline{\phi_\beta}:\overline{D_\beta}\to\overline{C}$ defined over $\mathbb{F}_p$. Furthermore we know that $\overline{D_\beta}$ is non-singular since the reduction of the matrix of partial derivatives in (3.3) has full rank. ☐

**Proposition 3.12.** *The genus $G$ of the covers $D_\alpha$ is equal to $q^{d-2}\left(\frac{d(q-1)}{2}-q\right)+1$.*

*Proof.* Let $\psi: C\to\mathbb{P}^1$ be the map $(X,Y,Z)\mapsto(X,Z)$. This has degree $q$ and is ramified above the $d$ points $(X,Z)$ satisfying $F(X,Z)=0$. Since $\phi_\alpha$ is unramified of degree $q^{d-2}$, the composition $\psi\circ\phi_\alpha : D_\alpha\to\mathbb{P}^1$ has degree $q^{d-1}$ and is ramified at the same points as $\psi$. Each ramification point has exactly $q^{d-2}$ preimages, each of them with ramification index $q$. The Riemann-Hurwitz formula applied to $\psi\circ\phi_\alpha$ yields

$$\begin{aligned}2G-2 =&(2\operatorname{Genus}(\mathbb{P}^1)-2)\deg(\psi\circ\phi_\alpha)+\sum_{P\in\mathbb{P}^1, Q\in(\psi\circ\phi_\alpha)^{-1}(P)}(e_Q-1)\\ 2G-2 =&-2q^{d-1}+dq^{d-2}(q-1)\\ G =&q^{d-2}\left(\frac{d(q-1)}{2}-q\right)+1\end{aligned}$$

☐

**Definition 3.13.** Define the set of ***useful primes*** to be

$$S_{up} := \left\{ p \text{ rational prime } : p \mid q\Delta \quad \text{or} \quad \sqrt{p} + \frac{1}{\sqrt{p}} \leq 2G \right\}.$$

**Proposition 3.14.** *Suppose that $p$ is a rational prime and $p \notin S_{up}$. Then $\bar{H}_{\mathbb{Q}}(\mathbf{S}) \subseteq r_p^{-1}\left(\mathrm{Image}(\mu_{\mathbb{Q}_p})\right)$.*

*Proof.* Let $\alpha \in A^*_{\mathbb{Q}}$ such that $[\alpha] \in \bar{H}_{\mathbb{Q}}(\mathbf{S})$ and $\beta \in A^*_{\mathbb{Q}_p}$ such that $[\beta] = r_p([\alpha])$. By Propositions 3.11 and 3.12 we know that $\overline{D_\beta}$ is a non-singular curve of genus $G$ over $\mathbb{F}_p$. Then by the Hasse-Weil inequality we have that $\#\overline{D_\beta}(\mathbb{F}_p) > 0$ and we can use Hensel's Lemma to lift to a point in $D_\beta(\mathbb{Q}_p)$. By Proposition 3.8 this is equivalent to $[\beta] = r_p([\alpha]) \in \mathrm{Image}(\mu_{\mathbb{Q}_p})$. □

**Corollary 3.15.**

$$\mathrm{Sel}^{(\mu)}(C, \mathbb{Q}) = \{\alpha \in H_{\mathbb{Q}} : r_p(\alpha) \in \mathrm{Image}(\mu_{\mathbb{Q}_p}) \textit{ for all } p \in S_{up}\}$$

3.3. **Computational efficiency.** The groups $A(q, \mathbf{S})$, $\mathbb{Q}(q, T)$ and the homomorphism $\iota$ defined in Sections 2.2 and 2.4 can be computed using commands implemented by Claus Fieker in the MAGMA computer algebra system [3], so we can compute $\pi_{\mathbb{Q}}(H_{\mathbb{Q}}(\mathbf{S})) = \bar{H}_{\mathbb{Q}}(\mathbf{S})$. The bottleneck of the computation is computing the class and unit groups of the number fields $K_h$, for $h \in \mathcal{F}_{\mathbb{Q}}$, which are needed for the construction of $A(q, \mathbf{S})$.

Also although Corollary 3.15 indicates that the algorithm computes $\mathrm{Sel}^{(\mu)}(C, \mathbb{Q})$ in a finite amount of time, the size of $S_{up}$ is prohibitively large and in general we can only hope to get information using small primes. Nevertheless we can still put the algorithm in good use as in most cases bigger primes do not have a contribution in cutting down the set we already have.

## 4. EXAMPLES

In this section we give examples of how descent on superelliptic curves can be used to tackle some interesting number theoretical problems. Example 4.1 is a preparatory example to demonstrate how the results from the local computations are obtained and combined to prove statements regarding the sets of rational points of the curve, or curves in question. In Example 4.2 we show how descent can sometimes be the appropriate technique for solving generalized Fermat equations. In Example 4.3 we consider a superelliptic curve, which although covers a plane cubic curve in an obvious way ($X \mapsto X^2, Z \mapsto Z^2$), the set of rational points of this curve is infinite, so it is impossible to construct the set of rational points of the superelliptic curve by pulling back rational points of the cubic curve. After using the algorithm described above we exclude all but one of the covers $D_\alpha$ due to local insolubility and we manage to compute all the rational points of this remaining cover $D_1$ by other means (found in [4],[5]). Finally, we compute $C(\mathbb{Q})$ since $C(\mathbb{Q}) = \phi_1(D_1(\mathbb{Q}))$. The reasoning of this example, i.e. using covering techniques to transfer the problem to a different type of curves, is also used in the proof of Theorem 4.5, but unlike Example 4.3, all the curves involved can be defined over $\mathbb{Q}$. Theorem 4.5 also demonstrates the significance of extending descent arguments to singular superelliptic curves.

**Example 4.1.** Consider the curve defined by the equation

$$y^5 = 2x^5 + x^4 + 2x^3 + x^2 + 3x + 3.$$

This is ELS, but after applying the algorithm to this curve we obtain the results shown in Table 1.

| $p$ | 1 | 2 | 3 | 5 … 17 | 19 … 37 | 41 |
|---|---|---|---|---|---|---|
| $\#\bar{H}_{\mathbb{Q}}(\mathbf{S}) \bigcap\limits_{\substack{l \text{ prime} \\ l \leq p}} r_l^{-1}(\mu_{\mathbb{Q}_l}(C(\mathbb{Q}_l)))$ | 25 | 25 | 25 | 2 … 2 | 1 … 1 | 0 |

TABLE 1. Descent computation for $C : y^5 = 2x^5 + x^4 + 2x^3 + x^2 + 3x + 3$.

Therefore

$$\bar{H}_{\mathbb{Q}}(\mathbf{S}) \cap r_5^{-1}\left(\mu_{\mathbb{Q}_5}(C(\mathbb{Q}_5))\right) \cap r_{19}^{-1}\left(\mu_{\mathbb{Q}_{19}}(C(\mathbb{Q}_{19}))\right) \cap r_{41}^{-1}\left(\mu_{\mathbb{Q}_{41}}(C(\mathbb{Q}_{41}))\right) = \emptyset$$

which proves that $C(\mathbb{Q}) = \emptyset$.

**Example 4.2.** In [9], Halberstadt and Kraus, consider the following four generalized Fermat equations

$$16a^7 + 87b^7 + 625c^7 = 0 \tag{4.1}$$

$$11a^5 + 29b^5 + 81c^5 = 0 \tag{4.2}$$

$$27a^5 + 16b^5 + 2209c^5 = 0 \tag{4.3}$$

$$32a^7 + 81b^7 + 187c^7 = 0 \tag{4.4}$$

These have solutions everywhere locally, but appear to have no rational points. The authors explain how the modular approach fails to show that the set of rational points is empty. We show how one can use descent to tackle all four of them.

Observe that the problem can be easily transferred to the one of finding rational points on superelliptic curves.

$$(4.1) \Leftrightarrow (-b, 2a, -c) \in C_1(\mathbb{Q}), \text{ where } C_1 : Y^7 = 8(87X^7 + 625Z^7)$$

$$(4.2) \Leftrightarrow (-a, 3c, -b) \in C_2(\mathbb{Q}), \text{ where } C_2 : Y^5 = 3(11X^5 + 29Z^5)$$

$$(4.3) \Leftrightarrow (-a, 2b, -c) \in C_3(\mathbb{Q}), \text{ where } C_3 : Y^5 = 2(27X^5 + 2209Z^5)$$

$$(4.4) \Leftrightarrow (-b, 2a, -c) \in C_4(\mathbb{Q}), \text{ where } C_4 : Y^7 = 4(81X^7 + 187Z^7)$$

Table 2 contains the results obtained when we perform descent on these curves.

| $p$ | 1 | 2 | 3 | 5 | 7 ... 23 | 29 |
|---|---|---|---|---|---|---|
| $\#\bar{H}_{\mathbb{Q}}(\mathbf{S}) \bigcap\limits_{\substack{l \text{ prime} \\ l \le p}} r_l^{-1}(\mu_{\mathbb{Q}_l}(C_1(\mathbb{Q}_l)))$ | 49 | 0 | | | | |
| $\#\bar{H}_{\mathbb{Q}}(\mathbf{S}) \bigcap\limits_{\substack{l \text{ prime} \\ l \le p}} r_l^{-1}(\mu_{\mathbb{Q}_l}(C_2(\mathbb{Q}_l)))$ | 0 | | | | | |
| $\#\bar{H}_{\mathbb{Q}}(\mathbf{S}) \bigcap\limits_{\substack{l \text{ prime} \\ l \le p}} r_l^{-1}(\mu_{\mathbb{Q}_l}(C_3(\mathbb{Q}_l)))$ | 5 | 5 | 5 | 1 | 1 ... 1 | 0 |
| $\#\bar{H}_{\mathbb{Q}}(\mathbf{S}) \bigcap\limits_{\substack{l \text{ prime} \\ l \le p}} r_l^{-1}(\mu_{\mathbb{Q}_l}(C_4(\mathbb{Q}_l)))$ | 7 | 0 | | | | |

TABLE 2. Results for the generalized Fermat curves

Therefore $C_i(\mathbb{Q}) = \emptyset$ for $i = 1, 2, 3, 4$.

**Example 4.3.** Consider the curve $C$ in $\mathbb{P}^2(1, 2, 1)$, defined by

$$(X, Y, Z) \in C \Leftrightarrow Y^3 = (X^2 - 3Z^2)(X^4 - 2Z^4).$$

This curve has three points at infinity $(1, 1, 0)$, $(1, \rho, 0)$ and $(1, \rho^2, 0)$, where $\rho$ is a primitive cube root of unity. So we know that it has at least one rational point. After applying the algorithm to this curve we obtain the results shown in Table 3.

The element of $\bar{H}_{\mathbb{Q}}(\mathbf{S})$ remaining is the image of the point $(1, 1, 0)$ under $\mu_{\mathbb{Q}}$ which is equal to the identity element $1\mathbb{Q}^* A^{*3}$. This corresponds to a cover $\phi_1 : D_1 \to C$, where $D_1$ is a curve in $\mathbb{P}^5 \times C$ defined as in (3.2), whose set of rational points is non-empty. We fix embeddings of $K_{(x^2-3)}$ and

| $p$ | 1 | 2 | 3 | 5 | 7 | 11 | 13 | 17 ... |
|---|---|---|---|---|---|---|---|---|
| $\#\bar{H}_{\mathbb{Q}}(\mathbf{S}) \bigcap_{\substack{l \text{ prime} \\ l \le p}} r_l^{-1}(\mu_{\mathbb{Q}_l}(C(\mathbb{Q}_l)))$ | 243 | 243 | 9 | 3 | 3 | 3 | 3 | 1 ... |

Table 3. Results for $C : y^3 = (x^2 - 3)(x^4 - 2)$.

$K_{(x^4-2)}$ in $\bar{\mathbb{Q}}$ and index the six elements of $\Theta_{\bar{\mathbb{Q}}}$ as $\vartheta_1 = \sqrt{3}, \vartheta_2 = -\sqrt{3}, \vartheta_3 = \sqrt[4]{2}, \vartheta_4 = -\sqrt[4]{2}, \vartheta_5 = i\sqrt[4]{2}$ and $\vartheta_6 = -i\sqrt[4]{2}$. $D_1$ is defined by the following relations

$$((u_1, \dots, u_6), (X, Y, Z)) \in D_1 \Leftrightarrow \exists \lambda \neq 0 \text{ such that } \quad \lambda u_j^3 = X - \vartheta_j Z \text{ for } 1 \le j \le 6 \text{ and } \lambda^2 \prod_{j=1}^{6} u_j = Y$$

This covers a curve $E'$ of genus 1 in $\mathbb{P}^2$, defined over the number field $L := \mathbb{Q}(\vartheta_3)$, given by the equation

$$(U, V, W) \in E' \Leftrightarrow \quad V^3 = (U - \vartheta_3 W)(U^2 + \vartheta_3^2 W^2).$$

We have the following commutative diagram

$$\begin{array}{ccccc} D_1 & \xrightarrow{\phi} & C & \quad ((u_1, \dots, u_6), (X, Y, Z)) & \longmapsto (X, Y, Z) \\ \kappa \downarrow & & \downarrow & \downarrow & \downarrow \\ E' & \xrightarrow[\tau]{} & \mathbb{P}^1 & \quad (Xu_3^2, (X - \vartheta_3 Z)u_5 u_6, Zu_3^2) & \longmapsto (X, Z) \end{array}$$

Note that $\kappa$ is a well defined rational map between two non-singular curves so it is actually a morphism. We can put $E'$ into Weierstrass form via a linear transformation, by moving the point $(\vartheta_3, 0, 1)$ to $\infty$. We obtain the Weierstrass model

$$E : y^2 z - 8\vartheta_3^2 y z^2 = x^3 - 64 z^3.$$

The isomorphism of the two models is given by

$$\psi : E \to E', \qquad \psi(x, y, z) = (\vartheta_3 y, 2\vartheta_3^3 x, y - 8\vartheta_3^2 z).$$

Using the package MAGMA we find that the Mordell-Weil rank of $E(L)$ is 1. Since

$$\tau\left(\kappa\left(\phi^{-1}(C(\mathbb{Q}))\right)\right) \subseteq \mathbb{P}^1(\mathbb{Q}),$$

we are not interested in all the $L$-rational points of $E'$, only $(U, V, W) \in E'(L)$ such that $U/W \in \mathbb{Q}$. Determining these will give us $C(\mathbb{Q})$. To solve this problem we can use "Elliptic curve Chabauty" [4]. Fortunately this is implemented in MAGMA. Using the inbuilt MAGMA commands we find that

$$\{(U, V, W) \in E'(L) : U/W \in \mathbb{Q}\} = \{(1, 1, 0), (0, -\vartheta_3, 1)\}.$$

We deduce that $C(\mathbb{Q}) = \{(1, 1, 0)\}$.

**Example 4.4.** In [2], [8], [11] and [13] the authors consider a generalization of Lucas "Square Pyramid" problem, namely the determination of all pairs $(a, b) \in \mathbb{Z}_{>0}^2$ that satisfy the equation

$$b^q = 1^k + 2^k + \ldots + a^k$$

for some $q \ge 2$ and $k \ge 1$. Theorem 4.5 below is already proved in [2] where the authors determine all the solutions for all values of $q$ and for $1 \le k \le 11$. It is suggested in [1] that this could have been extended to larger values of $k$. Nevertheless, we present here this special case since our proof, which involves descent, includes the determination of the full set of rational points (as opposed to the subset of integral points) of a singular superelliptic curve of genus 7. We prove the case with $q = 3$ because current tools only allow the use of cubic curves for the intermediate steps (although recent

developments, like the implementation of descent on $J_C$ in MAGMA, suggest that Chabauty's method for superelliptic curves should be available in the near future, which would open the possibility to solve cases with $q > 3$). We consider the case with $k = 9$ since this is a value of $k$ where the superelliptic curve involved in the computation is both singular and non-hyperelliptic.

**Theorem 4.5.** *The only pair* $(a, b) \in \mathbb{Z}^2_{>0}$ *satisfying*

$$b^3 = \sum_{i=1}^{a} i^9$$

*is* $(1, 1)$.

*Proof.* After replacing the right hand side of the equation by the closed formula for the sum of the first $a$ ninth powers we get the equation

$$b^3 = \frac{1}{10}a^2(a+1)^2(a^2+a-1)\left(a^4+2a^3-\frac{1}{2}a^2-\frac{3}{2}a+\frac{3}{2}\right) \tag{4.5}$$

After the change of variables in the proof of Proposition 2.3, we see that the solutions $(a, b)$ correspond to rational points on the following genus 7, singular, superelliptic curve $C$ in $\mathbb{P}^2(1, 4, 1)$

$$C:\ Y^3 = X^2(X+5Z)^2(X+10Z)^2(X^2+30XZ+100Z^2)(X^4+30X^3Z+460X^2Z^2+2400XZ^3+4000Z^4)$$

$$(a, b) \mapsto (10, 10000b, (a-1)) \in C(\mathbb{Q}) \tag{4.6}$$

We have the descent map $\mu_\mathbb{Q} : C(\mathbb{Q}) \to A^*_\mathbb{Q}/\mathbb{Q}^*A^{*3}_\mathbb{Q}$ where the algebra $A_\mathbb{Q}$ is isomorphic to the product $\mathbb{Q}\times\mathbb{Q}\times\mathbb{Q}\times K_1\times K_2$ where $K_1 = \mathbb{Q}[t]/(t^2+30t+100)$ and $K_2 = \mathbb{Q}[t]/(t^4+30t^3+460t^2+2400t+4000)$. Denote the images of $t$ in $K_1$ and $K_2$ by $\theta_1$ and $\theta_2$ respectively. We can compute representatives in $A^*_\mathbb{Q}$ for the images of the five known rational points. These are shown in Table 4.

| $i$ | $P_i \in C(\mathbb{Q})$ | $\mu_\mathbb{Q}(P_i)$ |
|---|---|---|
| 1 | $(1, 1, 0)$ | $[(1, 1, 1, 1, 1)]$ |
| 2 | $(0, 0, 1)$ | $[(1, 5, 10, \theta_1, \theta_2)]$ |
| 3 | $(-5, 0, 1)$ | $[(1, 75, 1, 1, 400(5\theta_2^3 + 134\theta_2^2 + 1860\theta_2 - 5840))]$ |
| 4 | $(-10, 0, 1)$ | $[(2, 1, 300, 25(3\theta_1 + 10), 20(\theta_2^3 + 20\theta_2^2 - 90\theta_2 - 700))]$ |
| 5 | $(-10, 1000, 3)$ | $[(2, 1, 4, 25(3\theta_1 + 10), 20(13\theta_2^3 + 330\theta_2^2 + 4380\theta_2 + 9600))]$ |

TABLE 4. Representatives in $A^*_\mathbb{Q}$ of images of known points.

By Proposition 3.12, the genus $G$ of the covers $D_\alpha$ is

$$G = q^{d-2}\left(\frac{d(q-1)}{2} - q\right) + 1 = 3^7\left(\frac{9\times 2}{2} - 3\right) + 1 = 13123$$

so the set $S_{up}$ (see Definition 3.13) contains the rational primes which are less than $4 \times 13123^2 = 688852516$. Performing the local computations for all of these primes would be unfeasible, but we do not need to, since after checking the primes 2, 3 and 5 we exclude every element from $H_\mathbb{Q}(\mathbf{S})$ apart from the five we already know. Thus

$$\mathrm{Sel}^{(\mu)}(C, \mathbb{Q}) = \mu_\mathbb{Q}(\{P_1, P_2, P_3, P_4, P_5\}).$$

These elements correspond to five covers $\phi_i : D_i \to C$, where each $D_i$ is a curve in $\mathbb{P}^8 \times C$, defined using a representative in $\mu_\mathbb{Q}(P_i)$ (see (3.2) in Section 3).

Now for each $1 \le i \le 5$, we choose a combination of three factors from $\mathcal{F}_{\bar{\mathbb{Q}}}$ to form a cover $\kappa_i : D_i \to E_i$ where $E_i$ is a genus one curve. By choosing factors whose product is defined over $\mathbb{Q}$, we ensure that $E_i$ and $\kappa_i$ are defined over $\mathbb{Q}$. When choosing the three factors we also aim to obtain an elliptic curve $E_i$ which has finitely many rational points. As it turns out, for all $1 \le i \le 5$, the subset $\{x, x+5, x+10\} \subseteq \mathcal{F}_{\bar{\mathbb{Q}}}$ satisfies the criteria we need, giving the five curves in Table 5.

| $i$ | $(U,V,W) \in E_i \Leftrightarrow$ | $\kappa_i\Big((u_h)_{h\in\mathcal{F}_{\bar{\mathbb{Q}}}},(X,Y,Z)\Big) =$ |
|---|---|---|
| 1 | $V^3 = U(U+5W)(U+10W)$ | $\Big(Xu_{(x)}^2, Xu_{(x+5)}u_{(x+10)}, Zu_{(x)}^2\Big)$ |
| 2 | $50V^3 = U(U+5W)(U+10W)$ | $\Big(Xu_{(x)}^2, Xu_{(x+5)}u_{(x+10)}, Zu_{(x)}^2\Big)$ |
| 3 | $75V^3 = U(U+5W)(U+10W)$ | $\Big(Xu_{(x)}^2, Xu_{(x+5)}u_{(x+10)}, Zu_{(x)}^2\Big)$ |
| 4 | $600V^3 = U(U+5W)(U+10W)$ | $\Big(Xu_{(x)}^2, Xu_{(x+5)}u_{(x+10)}, Zu_{(x)}^2\Big)$ |
| 5 | $8V^3 = U(U+5W)(U+10W)$ | $\Big(Xu_{(x)}^2, Xu_{(x+5)}u_{(x+10)}, Zu_{(x)}^2\Big)$ |

TABLE 5. The cubic curves $E_i$ and the maps $\kappa_i : D_i \to E_i$.

We note that there are isomorphisms $E_1 \cong E_5$ and $E_3 \cong E_4$ over $\mathbb{Q}$, but this is not relevant to the computation. We leave the coefficients of $V^3$ in $E_4$ and $E_5$ unchanged to remind the reader that they originate from multiplying the first three entries of the representatives of $\mu_{\mathbb{Q}}(P_i)$ shown in Table 4. All five cubic curves are elliptic curves with Mordell-Weil rank equal to 0 so we can determine the sets $E_i(\mathbb{Q})$.

$$E_1(\mathbb{Q}) = \left\{ \begin{array}{c} (0,0,1), (-10,-10,3), (-20,10,3), \\ (-10,0,1), \boxed{(1\ ,\ 1\ ,\ 0)}, (-5,0,1) \end{array} \right\}$$

$$E_2(\mathbb{Q}) = \left\{ \boxed{(0\ ,\ 0\ ,\ 1)}, (-10,0,1), (-5,0,1) \right\}$$

$$E_3(\mathbb{Q}) = \left\{ (0,0,1), (-10,0,1), \boxed{(\text{-}5\ ,\ 0\ ,\ 1)} \right\}$$

$$E_4(\mathbb{Q}) = \left\{ (0,0,1), \boxed{(\text{-}10\ ,\ 0\ ,\ 1)}, (-5,0,1) \right\}$$

$$E_5(\mathbb{Q}) = \left\{ \begin{array}{c} (0,0,1), (-10,0,1), (-5,0,1), \\ (-20,5,3), (2,1,0), \boxed{(\text{-}10\ ,\ \text{-}5\ ,\ 3)} \end{array} \right\}$$

We then compute the pre-images of these sets under the maps $\kappa_i$. The box indicates that a point has one $\mathbb{Q}$-rational point in its $\kappa_i$-fiber. The rest of the points have no rational pre-image. As expected, $D_i(\mathbb{Q})$ contains exactly one element for each $1 \le i \le 5$. Using Corollary 3.9 we get

$$C(\mathbb{Q}) = \bigcup_{i=1}^{5} \phi_i\left(D_i(\mathbb{Q})\right) = \{P_1, P_2, P_3, P_4, P_5\}.$$

These points correspond to all solutions $(a,b) \in \mathbb{Q}^2$ satisfying Equation (4.5). In particular, using the inverse of the map (4.6) we get that $P_1, P_2, P_3, P_4$ and $P_5$ correspond to $(1,1)$, "$\infty$", $(-1,0)$, $(0,0)$ and $(-2,1)$ respectively. Therefore $(1,1)$ is the only solution where both $a$ and $b$ are positive integers. □


## ACKNOWLEDGEMENTS

The author would like to thank Samir Siksek for his valuable comments and guidance, Dino Lorenzini for pointing out that descent would be applicable to the equations in Example 4.2 and Brendan Creutz along with the rest of the Computational Algebra Group at the University of Sydney, for their excellent hospitality and the opportunity to include the algorithms described in this paper in MAGMA [3].


## REFERENCES


1. Michael A. Bennett, *A superelliptic equation involving alternating sums of powers*, Publ. Math. Debrecen **79** (2011), no. 6.
2. Michael A. Bennett, Kálmán Győry, and Ákos Pintér, *On the Diophantine equation* $1^k + 2^k + \cdots + x^k = y^n$, Compos. Math. **140** (2004), no. 6, 1417–1431. MR 2098395 (2005g:11042)

3. Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478
4. Nils Bruin, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. **562** (2003), 27–49. MR 2011330 (2004j:11051)
5. Nils Bruin and E. Victor Flynn, *Towers of 2-covers of hyperelliptic curves*, Trans. Amer. Math. Soc. **357** (2005), no. 11, 4329–4347. MR 2156713 (2006k:11118)
6. Nils Bruin and Michael Stoll, *Two-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), no. 268, 2347–2370. MR 2521292 (2010e:11059)
7. Brendan Creutz, *Explicit descent in the Picard group of a cyclic cover of the projective line*, (2012), arXiv:1204.5803.
8. K. Győry, R. Tijdeman, and M. Voorhoeve, *On the equation* $1^k + 2^k + \cdots + x^k = y^z$, Acta Arith. **37** (1980), 233–240. MR 598878 (82h:10021)
9. Emmanuel Halberstadt and Alain Kraus, *Courbes de Fermat: résultats et problèmes*, J. Reine Angew. Math. **548** (2002), 167–234. MR 1915212 (2003h:11068)
10. Dino Lorenzini and Thomas J. Tucker, *Thue equations and the method of Chabauty-Coleman*, Invent. Math. **148** (2002), no. 1, 47–77. MR 1892843 (2003d:11088)
11. Ákos Pintér, *On the power values of power sums*, J. Number Theory **125** (2007), no. 2, 412–423. MR 2332596 (2008g:11052)
12. Bjorn Poonen and Edward F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. **488** (1997), 141–188. MR 1465369 (98k:11087)
13. Juan J. Schäffer, *The equation* $1^p + 2^p + 3^p + \cdots + n^p = m^q$, Acta Math. **95** (1956), 155–189. MR 0078395 (17,1187a)
14. Samir Siksek and Michael Stoll, *Partial descent on hyperelliptic curves and the generalized fermat equation* $x^3 + y^4 + z^5 = 0$, Bulletin of the London Mathematical Society **44** (2012), no. 1, 151–166.
15. Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094 (2010i:11005)


*E-mail address*: `M.Mourao@warwick.ac.uk`

MATHEMATICS INSTITUTE, UNIVERSITY OF WARWICK